EC-Council Certified Ethical Hacker (CEH) v.11

Summary

Length: 40 hours Level: Experienced

The Certified Ethical Hacker (CEH) credential is the most trusted ethical hacking certification and accomplishment recommended by employers globally. It is the most desired information security certification and represents one of the fastest-growing cyber credentials required by critical infrastructure and essential service providers. Since the introduction of CEH in 2003, it is recognized as a standard within the information security community. CEH v11 continues to introduce the latest hacking techniques and the most advanced hacking tools and exploits used by hackers and information security professionals today. The Five Phases of Ethical Hacking and the original core mission of CEH remain valid and relevant today: “To beat a hacker, you need to think like a hacker". This course may earn a Credly badge.

Learning Objectives

You will learn:

Key issues include plaguing the information security world, ethical hacking, information security controls, laws, and standards.
Perform footprinting and reconnaissance using the latest footprinting techniques and tools as a critical pre-attack phase required in ethical hacking.
Network scanning techniques and scanning countermeasures.
Enumeration techniques and enumeration countermeasures.
Vulnerability analysis to identify security loopholes in the target organization’s network, communication infrastructure, and end systems.
System hacking methodology, steganography, steganalysis attacks, and covering tracks to discover system and network vulnerabilities.
Different types of malware (Trojan, Virus, worms, etc.), system auditing for malware attacks, malware analysis, and countermeasures.
Packet sniffing techniques to discover network vulnerabilities and countermeasures to defend sniffing.
Social engineering techniques and how to identify theft attacks to audit human-level vulnerabilities and suggest social engineering countermeasures.
DoS/DDoS attack techniques and tools to audit a target and DoS/DDoS countermeasures.
Session hijacking techniques to discover network-level session management, authentication/authorization, cryptographic weaknesses, and countermeasures.
Web server attacks and a comprehensive attack methodology to audit vulnerabilities in web server infrastructure, and countermeasures.
Web application attacks and comprehensive web application hacking methodology to audit vulnerabilities in web applications, and countermeasures.
SQL injection attack techniques, injection detection tools to detect SQL injection attempts, and countermeasures.
Wireless encryption, wireless hacking methodology, wireless hacking tools, and Wi-Fi security tools.
Mobile platform attack vector, android vulnerability exploitations, and mobile security guidelines and tools.
Firewall, IDS and honeypot evasion techniques, evasion tools and techniques to audit a network perimeter for weaknesses, and countermeasures.
Cloud computing concepts (Container technology, serverless computing), various threats/attacks, and security techniques and tools.
Penetration testing, security audit, vulnerability assessment, and penetration testing roadmap.
Threats to IoT and OT platforms and learn how to defend IoT and OT devices securely.
Cryptography ciphers, Public Key Infrastructure (PKI), cryptography attacks, and cryptanalysis tools.

Course Outline

1. Course Outline

   Introduction to Ethical Hacking
   Footprinting and Reconnaissance
   Scanning Networks
   Enumeration
   Vulnerability Analysis
   System Hacking
   Malware Threats

Sniffing
Social Engineering
Denial-of-Service
Session Hijacking
Evading IDS, Firewalls, and Honeypots
Hacking Web Servers
Hacking Web Applications
SQL Injection
Hacking Wireless Networks
Hacking Mobile Platforms
IoT and OT Hacking
Cloud Computing
Cryptography

Audience

This course is ideal for those whose job role could be Information Security Analyst / Administrator, Information Assurance (IA) Security Officer, Information Security Manager / Specialist, Information Systems Security Engineer / Manager, Information Security Professionals / Officers, Information Security / IT Auditors, Risk / Threat/Vulnerability Analyst, System Administrators, and Network Administrators and Engineers.

Prerequisites

To be eligible to challenge the EC-Council CEH certification examination, the candidate has two options: Attend Official Network Security Training by EC-Council: If a candidate has completed an official EC-Council training either at an Accredited Training Center, via the iClass platform, or at an approved academic institution, the candidate is eligible to challenge the relevant EC-Council exam without going through the application process. Attempt the Exam without Official EC-Council Training: In order to be considered for the EC-Council CEH exam without attending official network security training, the candidate must have at least 2 years of work experience in the Information Security domain. If the candidate has the required work experience, they can submit an eligibility application form along with USD 100.00, a non-refundable fee.